

THE COMBINATORIAL NULLSTELLENSÄTZE REVISITED

PETE L. CLARK

ABSTRACT. We revisit and further explore the celebrated Combinatorial Nullstellensätze of N. Alon in several different directions.

Terminology: Throughout this note, a “ring” is a commutative ring with multiplicative identity. A “domain” is a ring R such that for all $a, b \in R \setminus \{0\}$, $ab \neq 0$. A ring R is “reduced” if for all $x \in R$ and $n \in \mathbb{Z}^+$, if $x^n = 0$ then $x = 0$.

1. INTRODUCTION

1.1. The Combinatorial Nullstellensätze.

This note concerns the following celebrated results of N. Alon.

Theorem 1. *Let F be a field, let $X_1, \dots, X_n \subset F$ be nonempty and finite, and $X = \prod_{i=1}^n X_i$. For $1 \leq i \leq n$, put*

$$(1) \quad \varphi_i(t_i) = \prod_{x_i \in X_i} (t_i - x_i) \in F[t_i] \subset F[t] = F[t_1, \dots, t_n].$$

Let $f \in F[t]$ be a polynomial which vanishes on all the common zeros of $\varphi_1, \dots, \varphi_n$: that is, for all $x \in F^n$, if $\varphi_1(x) = \dots = \varphi_n(x) = 0$, then $f(x) = 0$. Then:

*a) (Combinatorial Nullstellensatz I, or **CNI**) There are $q_1, \dots, q_n \in F[t]$ such that*

$$(2) \quad f(t) = \sum_{i=1}^n q_i(t) \varphi_i(t).$$

b) (Supplementary Relations) Let R be the subring of F generated by the coefficients of f and $\varphi_1, \dots, \varphi_n$. Then the q_1, \dots, q_n may be chosen to lie in $R[t]$ and satisfy

$$(3) \quad \forall 1 \leq i \leq n, \deg q_i \leq \deg f - \deg \varphi_i.$$

Theorem 2. *(Combinatorial Nullstellensatz II, or **CNII**) Let F be a field, $n \in \mathbb{Z}^+$, $a_1, \dots, a_n \in \mathbb{N}$, and let $f \in F[t] = F[t_1, \dots, t_n]$. We suppose:*

(i) $\deg f \leq a_1 + \dots + a_n$.

(ii) The coefficient of $t_1^{a_1} \dots t_n^{a_n}$ in f is nonzero.

Then, for any subsets X_1, \dots, X_n of F with $\#X_i = a_i + 1$ for $1 \leq i \leq n$, there is $x = (x_1, \dots, x_n) \in X = \prod_{i=1}^n X_i$ such that $f(x) \neq 0$.

Alon used his Combinatorial Nullstellensätze to derive various old and new results in number theory and combinatorics, starting with Chevalley’s Theorem that a homogeneous polynomial of degree d in at least $d + 1$ variables over a finite field has a nontrivial zero. The use of polynomial methods has burgeoned to a remarkable degree in recent years. We recommend the recent survey [Ta13], which lucidly describes the main techniques but also captures the sense of awe and excitement at the

extent to which these very simple ideas have cracked open the field of combinatorial number theory and whose range of future applicability seems almost boundless.

Of Theorems 1 and 2, Theorem 1 is stronger: one easily deduces CNII from CNI and the Supplementary Relations, but (apparently) not conversely. On the other hand, for applications in combinatorics and number theory, CNII seems more useful: [Al99] organizes its applications into seven different sections, and only in the last section is CNI applied. Later works have followed this trend to an even larger degree, to the extent that most later works simply refer to Theorem 2 as the Combinatorial Nullstellensatz. We find this trend somewhat unfortunate: on the one hand, CNI is the stronger result and does have *some* applications in its own right. On the other hand, it is CNI which is really a Nullstellensatz in the sense of algebraic geometry, and we find this geometric connection interesting and suggestive.

Recently attention has focused on the following sharpening of CNII due to Schauz, Lason and Karasev-Petrov [Sc08, Thm. 3.2], [La10, Thm. 3], [KP12, Thm. 4]).

Theorem 3. (*Coefficient Formula*) *Let F be a field, and let $f \in F[t]$. Let $a_1, \dots, a_n \in \mathbb{N}$ be such that $\deg f \leq a_1 + \dots + a_n$. For each $1 \leq i \leq n$, let $X_i \subset F$ with $\#X_i = a_i + 1$, and let $X = \prod_{i=1}^n X_i$. Let $d = (a_1, \dots, a_n)$, and let c_d be the coefficient of $t_1^{a_1} \dots t_n^{a_n}$ in f . Then*

$$(4) \quad c_d = \sum_{x=(x_1, \dots, x_n) \in X} \frac{f(x)}{\prod_{i=1}^n \varphi'_i(x_i)}.$$

In this note we revisit and further explore these theorems, in three different ways:

- In § 2 we improve CNI to a **Finitesatz** (Theorem 7): a full Nullstellensatz for polynomial functions on finite subsets of F^n over an arbitrary field F . When F is finite we recover the **Finite Field Nullstellensatz** of G. Terjanian (Corollary 8).
- In §3 we expose the close relation between Theorem 3 and Chevalley's original proof of Chevalley's Theorem. Adapting Chevalley's method gives a version of Theorem 3 valid over *any* ring R subject to an additional condition on X which always holds over a field. This generalization is due to U. Schauz [Sc08]. The main novelty here is our exposition of these results following Chevalley's original arguments. However, when we close up this circle of ideas we find that it yields a **Restricted Variable Chevalley-Warning Theorem** (Theorem 17). Restricted variable versions of Chevalley's Theorem and Warning's Second Theorem have recently appeared in the literature [Br11], [CFS14], so Theorem 17 is in some sense the last piece of the "Chevalley-to-Alon" conversion process.
- In §4 we further analyze the evaluation map from polynomials to function on an arbitrary subset $X \subset R^n$ for an arbitrary ring. Our results are far from definitive, and one of our main goals of this section is to show that the (perhaps rather arid-looking) formalism of a restricted variable Nullstellensatz leads naturally to some interesting open problems in polynomial interpolation over commutative rings.

2. A NULLSTELLENSATZ FOR FINITELY RESTRICTED POLYNOMIAL FUNCTIONS

2.1. Alon's Nullstellensatz versus Hilbert's Nullstellensatz.

The prospect of improving Theorem 1 *as a Nullstellensatz* has not been explored, perhaps because the notion of a Nullstellensatz, though seminal in algebra and geometry, is less familiar to researchers in combinatorics. But it was certainly familiar to Alon, who began [Al99] by recalling the following result.

Theorem 4. (*Hilbert's Nullstellensatz*) *Let F be an algebraically closed field, let $g_1, \dots, g_m \in F[t]$, and let $f \in F[t]$ be a polynomial which vanishes on all the common zeros of g_1, \dots, g_m . Then there is $k \in \mathbb{Z}^+$ and $q_1, \dots, q_m \in F[t]$ such that*

$$f^k = \sum_{i=1}^m q_i g_i.$$

Let us compare Theorems 1 and 4. They differ in the following points:

- In Theorem 1, F can be any field. In Hilbert's Nullstellensatz, F must be algebraically closed. Really must: if not, there is a nonconstant polynomial $g(t_1)$ without roots in F ; taking $m = 1$, $g_1 = g$ and $f = 1$, the conclusion fails.
- In CNI, the conclusion is that f itself is a linear combination of the φ_i 's with polynomial coefficients, but in Hilbert's Nullstellensatz we must allow taking a power of f . Really must: e.g. take $k \in \mathbb{Z}^+$, $m = 1$, $g_1 = t_1^k$ and $f = t_1$.
- The Supplementary Relations give upper bounds on the degrees of the polynomials q_i : they make CNI **effective**. Hilbert's Nullstellensatz is not effective. Effective versions have been given by Brownawell [Br87], Kollár [Ko88] and others, but their bounds are much more complicated than the ones in Theorem 1.
- In Theorem 1 the φ_i 's are extremely restricted. On the other hand, in Hilbert's Nullstellensatz the g_i 's can be any set of polynomials. Thus Theorem 4 is a *full Nullstellensatz*, whereas Theorem 1 is a *partial Nullstellensatz*.

We will promote Theorem 1 to a full Nullstellensatz for all finite subsets.

2.2. The Restricted Variable Formalism.

In this section we give the formalism for a Nullstellensatz in the restricted variable context. Although our main theorem applies to finite subsets of affine n -space over a field, it is possible to set things up more generally, and doing so raises some further interesting questions and will be seen to have some useful applications.

For a set Z , let 2^Z be the set of all subsets of Z . For a ring R , let $\mathcal{I}(R)$ be the set of ideals of R . For a subset J of a ring R , let $\langle J \rangle$ denote the ideal of R generated by J , and let $\text{rad } J = \text{rad } \langle J \rangle$ denote the set of all $f \in R$ such that $f^k \in \langle J \rangle$ for some $k \in \mathbb{Z}^+$. An ideal J is **radical** if $J = \text{rad } J$.

Let R be a ring, and let $X \subset R^n$. For $x \in X$, $f \in R[t]$, we put

$$I(x) = \{f \in R[t] \mid f(x) = 0\},$$

$$V_X(f) = \{x \in X \mid f(x) = 0\}.$$

Put $V = V_{R^n}$. We may extend I and V_X to maps on power sets as follows:

$$I : 2^X \rightarrow 2^{R[t]}, \quad A \subset X \mapsto I(A) = \bigcap_{a \in A} I(a) = \{f \in R[t] \mid \forall a \in A, f(a) = 0\},$$

$$V_A : 2^{R[t]} \rightarrow 2^X, \quad J \subset R[t] \mapsto V_A(J) = \bigcap_{f \in J} V_A(f) = \{x \in X \mid \forall f \in J, f(x) = 0\}.$$

Then in fact

$$I : 2^X \rightarrow \mathcal{I}(R[t]), \quad \forall J \subset R[t], \quad V(J) = V(\langle J \rangle).$$

The maps I and V_A are **antitone**:

$$A_1 \subset A_2 \subset X \implies I(A_1) \supset I(A_2),$$

$$J_1 \subset J_2 \subset R[t] \implies V_A(J_1) \supset V_A(J_2),$$

so their compositions are **isotone**:

$$A_1 \subset A_2 \subset X \implies V_X(I(A_1)) \subset V_X(I(A_2)),$$

$$J_1 \subset J_2 \subset R[t] \implies I(V_X(J_1)) \subset I(V_X(J_2)).$$

We have $X = V_X(0)$, so

$$\forall J \subset R[t], \quad I(V_X(J)) \supset I(V_X(0)) = I(X).$$

2.3. The Finitesatz.

Lemma 5. a) Suppose R is a domain. For all ideals J_1, \dots, J_m of $R[t]$, we have

$$V_X(J_1 \cdots J_m) = \bigcup_{i=1}^m V_X(J_i).$$

b) Suppose R is reduced. Then for all $A \subset R^n$, $I(A)$ is a radical ideal.

c) If R is reduced, then for all $J \subset R[t]$,

$$(5) \quad I(V_X(J)) \supset \text{rad}(J + I(X)) \supset \text{rad } J + I(X) \supset J + I(X).$$

Proof. a) We intend to allow $m = 0$, in which case the identity reads $V_X(\langle 1 \rangle) = \emptyset$, which is true. Having established that, we immediately reduce to the case $m = 2$. Since $J_1 J_2 \subset J_i$ for $i = 1, 2$, $V_X(J_1 J_2) \supset V_X(J_i)$ for $i = 1, 2$, thus $V_X(J_1 J_2) \supset V_X(J_1) \cup V_X(J_2)$. Now let $x \in X \setminus (V_X(J_1) \cup V_X(J_2))$. For $i = 1, 2$ there is $f_i \in J_i$ with $f_i(x) \neq 0$. Since R is a domain, $f_1(x)f_2(x) \neq 0$, so $x \notin V_X(J_1 J_2)$.

b) If $f \in R[t]$ and $f^k \in I(A)$ for some $k \in \mathbb{Z}^+$, then for all $x \in A$ we have $f(x)^k = 0$. Since R is reduced, this implies $f(x) = 0$ for all $x \in A$ and thus $f \in I(A)$.

c) $I(V_X(J)) = I(X \cap V(J))$ is a radical ideal containing both $I(X)$ and $I(V(J)) \supset J$, so it contains $\text{rad}(J + I(X))$. The other inclusions are immediate. \square

It is well known (see Theorem 11) that when F is infinite we have $I(F^n) = \{0\}$. This serves to motivate the following restatement of Hilbert's Nullstellensatz.

Theorem 6. Let F be an algebraically closed field. For all $J \subset F[t]$,

$$I(V(J)) = \text{rad } J.$$

Here is the main result of this section.

Theorem 7. (Finitesatz) Let F be a field, and let $X \subset F^n$ be a finite subset.

a) For all ideals J of $F[t]$, we have

$$(6) \quad I(V_X(J)) = J + I(X).$$

In particular, if $J \supset I(X)$ then $I(V_X(J)) = J$.

b) (CNI) Suppose $X = \prod_{i=1}^n X_i$ for finite nonempty subsets X_i of F . Define $\varphi_i(t_i) \in F[t_i]$ as in (1) above. Then

$$(7) \quad I(X) = \langle \varphi_1, \dots, \varphi_n \rangle.$$

Proof. a) Let F be a field, and let $X \subset F^n$ be finite. Let $x = (x_1, \dots, x_n) \in X$. Let $\mathfrak{m}_x = \langle t_1 - x_1, \dots, t_n - x_n \rangle$. Then $F[t]/\mathfrak{m}_x \cong F$, so \mathfrak{m}_x is maximal. On the other hand $\mathfrak{m}_x \subset I(x) \subsetneq F[t]$, so $\mathfrak{m}_x = I(x)$. Moreover $V_X(\mathfrak{m}_x) = \{x\}$, hence

$$I(V_X(\mathfrak{m}_x)) = I(x) = \mathfrak{m}_x.$$

Now let $A = \{x_i\}_{i=1}^k \subset X$. Then

$$I(A) = I\left(\bigcup_i \{x_i\}\right) = \bigcap_i I(x_i) = \bigcap_i \mathfrak{m}_{x_i},$$

so by the Chinese Remainder Theorem [L, Cor. 2.2],

$$F[t]/I(A) = F[t]/\bigcap_i \mathfrak{m}_{x_i} \cong \prod_i F[t]/\mathfrak{m}_{x_i} \cong F^{\#X}.$$

Let F^A be the set of all maps $f : A \rightarrow F$, so F^A is an F -algebra under pointwise addition and multiplication and $F^A \cong \prod_{i=1}^{\#A} F$. The **evaluation map**

$$E_A = F[t] \rightarrow F^A, \quad f \in F[t] \mapsto (x \in A \mapsto f(x))$$

is a homomorphism of F -algebras. Moreover $\text{Ker } E_A = I(A)$, so E_A induces a map

$$\iota : F[t]/I(A) \hookrightarrow F^A.$$

Thus ι is an injective F -linear map between F -vector of equal finite dimension, hence an isomorphism of rings. It follows that

$$\#\mathcal{I}(F[t]/I(X)) = \#\mathcal{I}(F^X) = 2^{\#X}.$$

By restricting V_X to ideals containing $I(X)$, we get maps

$$\begin{aligned} V_X : \mathcal{I}(F[t]/I(X)) &\rightarrow 2^X, \\ I : 2^X &\rightarrow \mathcal{I}(F[t]/I(X)). \end{aligned}$$

For all $A \subset X$, we have

$$V_X(I(A)) = V_X\left(\bigcap_{i=1}^k \mathfrak{m}_{x_i}\right) = \bigcup_{i=1}^k V_X(\mathfrak{m}_{x_i}) = \bigcup_{i=1}^k \{x_i\} = A.$$

Since $\mathcal{I}(F[t]/I(X))$ and 2^X have the same finite cardinality, it follows that V_X and I are mutually inverse bijections! Thus for any ideal J of $F[t]$, using (5) we get

$$J + I(X) \subset I(V_X(J)) \subset I(V_X(J + I(X))) = J + I(X).$$

b) Let $d_i = \deg \varphi_i$ and put $\Phi = \langle \varphi_1, \dots, \varphi_n \rangle$. Since $\varphi_i|_X \equiv 0$ for all i , $\Phi \subset \text{Ker } E$, so there is an induced surjective F -algebra homomorphism

$$\tilde{E}_X : F[t]/\Phi \rightarrow F[t]/\text{Ker } E_X \rightarrow F^X.$$

Since $F[t]/\Phi$ and F^X are F -vector spaces of dimension $d_1 \cdots d_n$, \tilde{E} is an isomorphism. Hence $F[t]/\Phi \rightarrow F[t]/\text{Ker } E$ is injective, i.e., $\Phi = \text{Ker } E = I(X)$. \square

Corollary 8. (Finite Field Nullstellensatz [Te66]) Let \mathbb{F}_q be a finite field. Then for all ideals J of $\mathbb{F}_q[t]$, we have $I(V_{\mathbb{F}_q^n}(J)) = J + \langle t_1^q - t_1, \dots, t_n^q - t_n \rangle$.

Proof. Apply Theorem 7 with $F = X_1 = \dots = X_n = \mathbb{F}_q$. \square

3. CYLINDRICAL REDUCTION AND THE ATOMIC FORMULA

3.1. From Chevalley to Alon.

The first application of CNII in [Al99] is to Chevalley's Theorem. But there is a tighter relationship: the technique Alon uses to prove CNI directly generalizes the technique that Chevalley used, a process which we call **cylindrical reduction**. Chevalley applies (his special case of) CNI to prove his theorem in a different way from Alon's deduction of CNII: whereas Alon uses Theorem 1b), Chevalley gives an explicit formula for a reduced polynomial in terms of its associated polynomial function. This **Atomic Formula** easily implies the Coefficient Formula, which in turn immediately implies CNII. Moreover, since the spirit of CNII is to deduce information about the coefficients of a polynomial from information about its values on a finite set, the Atomic Formula is really the natural result along these lines, as it literally recovers the polynomial from its values on a sufficiently large finite set. Thus we feel that researchers should have the Atomic Formula in their toolkits.

Our Atomic Formula is one of the “interpolation formulas” of a 2008 work of U. Schauz [Sc08, Thm. 2.5]. Unfortunately it seems that Schauz's work has not been properly appreciated. Thus in this section we attempt to present this material in a way which reveals it to be as simple and appealing as Chevalley's classic work.

3.2. Cylindrical Reduction.

Lemma 9. (*Polynomial Division*)

Let R be a ring, and let $a(t_1), b(t_1) \in R[t_1]$ with b monic of degree d .

- a) There are unique polynomials q and r with $a = qb + r$ and $\deg r < d$.
- b) Suppose $R = A[t_2, \dots, t_n]$ is itself a polynomial ring over a ring A , so $R[t_1] = A[t_1, \dots, t_n] = A[t]$ and that $b \in A[t_1]$. Then:
 - If q has a monomial term of multidegree (d_1, \dots, d_n) , then a has a monomial term of multidegree $(d_1 + d, d_2, \dots, d_n)$. It follows that

$$\deg a \leq \deg q + d.$$

- If r has a monomial term of multidegree (d_1, \dots, d_n) , then a has a monomial term of multidegree (e_1, \dots, e_n) with $d_i \leq e_i$ for all $1 \leq i \leq n$. It follows that

$$\deg r \leq \deg a.$$

Proof. a) Uniqueness: if $a = q_1b + r_1 = q_2b + r_2$, then since b is monic and $g_1 \neq g_2$ then we have $d \leq \deg((g_1 - g_2)b) = \deg(r_2 - r_1) < d$, a contradiction. Existence: when b is monic, the standard division algorithm involves no division of coefficients so works in any ring. Part b) follows by contemplating the division algorithm. \square

Proposition 10. (*Cylindrical Reduction*) Let R be a ring. For $1 \leq i \leq n$, let $\varphi_i(t_i) \in F[t_i]$ be monic of degree d_i . Put $\Phi = \langle \varphi_1, \dots, \varphi_n \rangle$ and $d = (d_1, \dots, d_n)$. Say $f \in R[t]$ is **d -reduced** if for all $1 \leq i \leq n$, $\deg_{t_i} f < d_i$. Then:

- a) The set \mathcal{R}_d of all d -reduced polynomials is a free R -module of rank $d_1 \cdots d_n$.
- b) For all $f \in R[t]$, there are $q_1, \dots, q_n \in R[t]$ such that $\deg q_i \leq \deg f - \deg \varphi_i$ and $f - \sum_{i=1}^n q_i \varphi_i$ is d -reduced.
- c) The composite map $\Psi : \mathcal{R}_d \hookrightarrow R[t] \rightarrow R[t]/\Phi$ is an R -module isomorphism.
- d) For all $f \in R[t]$, there is a unique $r_d(f) \in \mathcal{R}_d$ such that $f - r_d(f) \in \langle \varphi_1, \dots, \varphi_n \rangle$.

Proof. a) Indeed $\{t_1^{a_1} \cdots t_n^{a_n} \mid 0 \leq a_i < d_i\}$ is a basis for \mathcal{R}_d .

b) Divide f by φ_1 , then divide the remainder r_1 by φ_2 , then divide the remainder r_2 by φ_n , and so forth, getting $f = \sum_{i=1}^n q_i \varphi_i + r_n$. Apply Lemma 9b).

c) Part b) implies that Ψ is surjective. For the injectivity: let $q_1, \dots, q_n \in R[t]$ be such that $f = \sum_{i=1}^n q_i \varphi_i \in \mathcal{R}_d$. We must show that $f = 0$. For each i , by dividing q_i by φ_j for $i < j \leq n$ and absorbing the quotient into the coefficient q_j of φ_j , we may assume that $\deg_{t_j} q_i < d_j$ for all $j > i$. It now follows easily that for all $1 \leq m \leq n$, $\sum_{i=1}^n q_i \varphi_i$ is either 0 or has t_i -degree at least d_i for some $1 \leq i \leq m$. Applying this with $m = n$ shows $f = 0$.

d) This follows immediately from part c). \square

Let R be a ring, and let $X_1, \dots, X_n \subset R$ be finite and nonempty. For $1 \leq i \leq n$ let $\varphi_i(t_i)$ be as in (1) and put $\Phi = \langle \varphi_1, \dots, \varphi_n \rangle$. Put $a_i = \#X_i$ and $X = \prod_{i=1}^n X_i$. We say $f \in R[t]$ is **X-reduced** if it is (a_1, \dots, a_n) -reduced, and we write \mathcal{R}_X for \mathcal{R}_d . We have $\dim \mathcal{R}_d = \prod_{i=1}^n a_i = \#X$. The **X-reduced representative** of f is the unique polynomial $r_X(f)$ such that $f - r_X(f) \in \langle \varphi_1, \dots, \varphi_n \rangle$.

Let S be a subset of a ring R . We say S satisfies **Condition (F)** (resp. **Condition (D)**) if for all $x, y \in S$, $x \neq y \implies x - y \in R^\times$ (resp. $x - y$ is a non-zero-divisor in R : if $(x - y)z = 0$ then $z = 0$). Condition (F) implies Condition (D). Observe that R is a field iff every subset satisfies Condition (F), and R is a domain iff every subset satisfies Condition (D). If $X = \prod_{i=1}^n X_i \subset R^n$, we say X satisfies Condition (F) (resp. Condition (D)) if every X_i satisfies Condition (F) (resp. Condition (D)).

Theorem 11. (CATS Lemma [Ch35] [AT92], [Sc08]) *Let R be a ring. For $1 \leq i \leq n$, let $X_i \subset R$ be nonempty and finite. Put $X = \prod_{i=1}^n X_i$.*

a) (Schauf) The following are equivalent:

(i) X satisfies condition (D).

(ii) If $f \in \mathcal{R}_X$ and $f(x) = 0$ for all $x \in X$, then $f = 0$.

(iii) We have $\Phi = I(X)$.

b) (Chevalley-Alon-Tarsi) The above conditions always hold when R is a domain.

Proof. a) (i) \implies (ii): By induction on n : suppose $n = 1$. Write $X = \{x_1, \dots, x_{a_1}\}$, and let $f \in R[t_1]$ have degree less than $a_1 - 1$ such that $f(x_i) = 0$ for all $1 \leq i \leq a_1$. By Polynomial Division, we can write $f = (t_1 - x_1)f_2$ for $f_2 \in R[t_1]$. Since $x_2 - x_1$ is not a zero-divisor, $f_2(x_2) = 0$, so $f_2(t_1) = (t_1 - x_2)$. Proceeding in this manner we eventually get $f(t_1) = (t_1 - x_1) \cdots (t_1 - x_{a_1})f_{a_1+1}(t_1)$, and comparing degrees shows $f = 0$. Suppose $n \geq 2$ and that the result holds in $n - 1$ variables. Write

$$f = \sum_{i=0}^{a_n-1} f_i(t_1, \dots, t_{n-1}) t_n^i$$

with $f_i \in R[t_1, \dots, t_{n-1}]$. If $(x_1, \dots, x_{n-1}) \in \prod_{i=1}^{n-1} X_i$, then $f(x_1, \dots, x_{n-1}, t_n) \in R[t_n]$ has degree less than a_n and vanishes for all a_n elements $x_n \in X_n$, so it is the zero polynomial: $f_i(x_1, \dots, x_{n-1}) = 0$ for all $0 \leq i \leq a_n$. By induction, each $f_i(t_1, \dots, t_{n-1})$ is the zero polynomial and thus f is the zero polynomial.

(ii) \implies (iii): Certainly $\Phi \subset I(X)$. Let $f \in I(X)$. Since $f - r_X(f) \in \Phi \subset I(X)$, for all $x \in X$ we have $r_X(f) = f(x) = 0$. Then (i) gives $r_X(f) = 0$ and thus $f \in \Phi$.

(iii) \implies (i): We argue by contraposition: suppose X does not satisfy Condition (D). Then for some $1 \leq i \leq n$, we may write $X_i = \{x_1, x_2, \dots, x_{a_i}\}$ such that there is $0 \neq z \in R$ with $(x_1 - x_2)z = 0$. Then $f = z(t_i - x_2)(t_i - x_3) \cdots (t_i - x_{a_i})$ is a

nonzero element of $I(X) \cap \mathcal{R}_X$, hence $f \in I(X) \setminus \Phi$.

b) If R is a domain then Condition (D) holds for every X . \square

Suppose F is a domain and $f \in F[t]$ vanishes on X . By Theorem 11 $f \in \Phi$, and thus by Proposition 10 there are $q_1, \dots, q_n \in F[t]$ with $\deg q_i \leq \deg f - a_i$ for all i such that $f - \sum_{i=1}^n q_i \varphi_i = r_X(f) = 0$, so $f = \sum_{i=1}^n q_i \varphi_i$. This proves Theorem 1b).

3.3. The Atomic Formula and the Coefficient Formula.

Lemma 12. *Suppose Condition (F). Let $x = (x_1, \dots, x_n) \in X$, and put*

$$\delta_{X,x} = \prod_{i=1}^n \prod_{y_i \in X_i \setminus \{x_i\}} \frac{t_i - y_i}{x_i - y_i} = \prod_{i=1}^n \frac{\varphi_i(t_i)}{(t_i - x_i)\varphi'_i(x_i)} \in F[t].$$

a) *We have $\delta_{X,x}(x) = 1$.*

b) *If $y \in X \setminus \{x\}$, then $\delta_{X,x}(y) = 0$.*

c) *For all $1 \leq i \leq n$, $\deg_{t_i} \delta_{X,x} = a_i - 1$. In particular, $\delta_{X,x}$ is X -reduced.*

Proof. Left to the reader. \square

Theorem 13. *(Atomic Formula) Suppose Condition (F). For all $f \in R[t]$, we have*

$$(8) \quad r_X(f) = \sum_{x \in X} f(x) \delta_{X,x}.$$

Proof. Apply Theorem 11a) to $r_X(f) - \sum_{x \in X} f(x) \delta_{X,x}$. \square

Let $d = (d_1, \dots, d_n) \in \mathbb{N}^d$. We say a polynomial $f \in F[t]$ is **d-topped** if for any $e = (e_1, \dots, e_n)$ with $d_i \leq e_i$ for all $1 \leq i \leq n$ and $\sum_{i=1}^n d_i < \sum_{i=1}^n e_i$, then the coefficient of $t^e = t_1^{e_1} \dots t_n^{e_n}$ in f is 0.

Remark 14. *If $\deg f \leq d_1 + \dots + d_n$, then f is d -topped.*

Lemma 15. *Let $d = (a_1 - 1, \dots, a_n - 1)$, and let $f \in F[t]$ be d -topped. Then the coefficient of $t^d = t_1^{a_1-1} \dots t_n^{a_n-1}$ in f is equal to the coefficient of t^d in $r_X(f)$.*

Proof. Write $\varphi_i(t_i) = t_i^{a_i} - \psi_i(t_i)$, $\deg(\psi_i) < a_i$. An **elementary cylindrical reduction** of f consists of identifying a monomial which is divisible by $t_i^{a_i}$ and replacing $t_i^{a_i}$ by $\psi_i(t_i)$. Elementary cylindrical reduction on a d -topped polynomial yields a d -topped polynomial with the same coefficient of t^d . The reduced polynomial $r_X(f)$ is obtained from f by finitely many elementary cylindrical reductions. \square

We deduce a *proof* of the Coefficient Formula (Theorem 3): by Remark 14, f is d -topped, so $c_d(f) = c_d(r_X(f))$. Apply (8).

Remark 16. *The proof shows that Theorem 3 holds with weaker hypotheses:*

(i) “ $\deg f \leq a_1 + \dots + a_n$ ” can be weakened to “ f is (a_1, \dots, a_n) -topped”.

(ii) “ F is a field” can be weakened to “ S satisfies Condition (F)”. It can be further weakened to “ S satisfies Condition (D)” so long as we interpret (4) as taking place in the total fraction ring of F (equivalently, if we clear denominators).

The first strengthening appears in the work of Schauz and Lasón and the second appears in the work of Schauz (see especially [Sc08, Thm. 2.9]).

3.4. The Restricted Variable Chevalley-Warning Theorem.

For a ring R and $x = (x_1, \dots, x_n) \in R^n$, we put $w(x) = \#\{1 \leq i \leq n \mid x_i \neq 0\}$.

Theorem 17. (*Restricted Variable Chevalley-Warning Theorem*) Let $P_1, \dots, P_r \in \mathbb{F}_q[t] = \mathbb{F}_q[t_1, \dots, t_n]$ be polynomials of degrees d_1, \dots, d_r . For $1 \leq i \leq n$, let $\emptyset \neq X_i \subseteq \mathbb{F}_q$ be subsets, put $X = \prod_{i=1}^n X_i$ and also

$$V_X = \{x = (x_1, \dots, x_n) \in X \mid P_1(x) = \dots = P_r(x) = 0\}.$$

Suppose that $(d_1 + \dots + d_r)(q-1) < \sum_{i=1}^n (\#X_i - 1)$. Then:

a) As elements of \mathbb{F}_q , we have

$$(9) \quad \sum_{x \in V_X} \frac{1}{\prod_{i=1}^n \varphi'_i(x_i)} = 0$$

and thus [Sc08] [Br11]

$$(10) \quad \#V_X \neq 1.$$

b) (*Chevalley-Warning*) If $\sum_{i=1}^r d_i < n$, then $p \mid \#\{x \in \mathbb{F}_q^n \mid P_1(x) = \dots = P_r(x)\}$.

c) (*Wilson*) If $(d_1 + \dots + d_r)(q-1) < n$, then

$$\#\{x \in V_{\{0,1\}^n} \mid w(x) \equiv 0 \pmod{2}\} \equiv \#\{x \in V_{\{0,1\}^n} \mid w(x) \equiv 1 \pmod{2}\} \pmod{p}.$$

d) If $(d_1 + \dots + d_r)(q-1) < (q-2)n$, then

$$\sum_{x \in \mathbb{F}_q^n \mid f_1(x) = \dots = f_r(x) = 0} x_1 \cdots x_n = 0.$$

Proof. a) We define

$$P(t) = \chi_{P_1, \dots, P_r}(t) = \prod_{i=1}^r (1 - P_i(t)^{q-1}),$$

so $\deg P = (q-1)(d_1 + \dots + d_r) < \sum_{i=1}^n (\#X_i - 1)$, and thus the coefficient of $t_1^{\#X_1-1} \dots t_n^{\#X_n-1}$ in P is 0. Applying the Coefficient Formula, we get

$$0 = \sum_{x \in X} \frac{P(x)}{\prod_{i=1}^n \varphi'_i(x_i)} = \sum_{x \in V_X} \frac{1}{\prod_{i=1}^n \varphi'_i(x_i)} \in \mathbb{F}_q.$$

Parts b) through d) follow from part a) by taking X to be, respectively, \mathbb{F}_q^n , $\{0, 1\}^n$ and $(\mathbb{F}_q^\times)^n$, and computing the $\varphi'_i(t_i)$'s. The details are left to the reader. \square

4. FURTHER ANALYSIS OF THE EVALUATION MAP

4.1. The Finitesatz holds only over a field.

If R is a ring which is not a field and $X \neq \emptyset$, then the assertion of Theorem 7a) remains meaningful with R in place of F , but it is false. Let $x \in X$. Since $F[t]/\mathfrak{m}_x \cong F$, \mathfrak{m}_x is *not* maximal, so let J be an ideal with $\mathfrak{m}_x \subsetneq J \subsetneq F[t]$, and let $f \in J \setminus \mathfrak{m}_x$. Then $V_X(J) \subset V_X(\mathfrak{m}_x) = \{x\}$, and since $f \notin \mathfrak{m}_x$, $f(x) \neq 0$. So

$$I(V_X(J)) = I(\emptyset) = F[t] \supsetneq J = J + I(X).$$

4.2. Towards an Infinitesatz.

We revisit the formalism of § 2.2: let R be a ring any $X \subset R^n$.

For a subset $A \subset R^n$ we define the **Zariski closure** $\overline{A} = V(I(A))$. Thus \overline{A} is the set of points at which any polynomial which vanishes at every point of A must also vanish. A subset A is **algebraic** if $A = \overline{A}$ and **Zariski-dense** if $\overline{A} = R^n$. When R is a domain the algebraic subsets are the closed sets of a topology, the **Zariski topology**. this need not hold and some strange things can happen: for instance if $R = \mathbb{Z}/6\mathbb{Z}$ and $n = 1$ then $\overline{\{2, 3\}} = \{0, 2, 3, 5\}$.

If F is an algebraically closed field and $X \subset F^n$ is algebraic, then using Hilbert's Nullstellensatz, for all ideals J of $F[t]$,

$$\begin{aligned} I(V_X(J)) &= I(V(J) \cap X) = I(V(J) \cap V(I(X))) \\ &= I(V(J \cup I(X))) = I(V(J + I(X))) = \text{rad}(J + I(X)). \end{aligned}$$

When X is infinite, we CLAIM the “rad” cannot be removed.

PROOF OF CLAIM: Suppose $\text{rad}(J + I(X)) = J + I(X)$ for all J . Equivalently, every ideal $J \supset I(X)$ is a radical ideal. Then for any element x the quotient ring $F[t]/I(X)$, since (x^2) is radical we must have $(x) = (x^2) = (x)^2$. It follows that $F[t]/I(X)$ is absolutely flat, hence has Krull dimension zero, hence Artinian, hence has finitely many maximal ideals. Since $x \mapsto \mathfrak{m}_x$ is an injection from X to the set of maximal ideals of $F[t]/I(X)$, X is finite.

The case of an arbitrary subset over an arbitrary ring R is much more challenging. In fact, even determining whether the evaluation map $E_X : R[t] \rightarrow R^X$ is surjective – **existence of interpolation polynomials** – or injective – **uniqueness of interpolation polynomials** – becomes nontrivial. In the next section we address these questions, but we are not able to resolve them completely.

4.3. Injectivity and Surjectivity of the Evaluation Map.

Lemma 18. *Let R be a ring. Let M_1 and M_2 be free R -modules, with bases \mathcal{B}_1 and \mathcal{B}_2 . If $\iota : M_1 \rightarrow M_2$ is an injective R -module map, then $\#\mathcal{B}_1 \leq \#\mathcal{B}_2$.*

Proof. Combine [LMR, Cor. 1.38] and [EMR, Ex. 1.24]. \square

Lemma 19. *Let R be a ring, and let X be an infinite set. Then R^X is not a countably generated R -module.*

Proof. Step 1: For $x \in \mathbb{R}$, let $A_x = \{y \in \mathbb{Q} \mid y < x\}$, and let $\mathcal{C}_{\mathbb{Q}} = \{A_x\}_{x \in \mathbb{R}}$. Then $\mathcal{C}_{\mathbb{Q}} \subset 2^{\mathbb{Q}}$ is an uncountable linearly ordered family of nonempty subsets of \mathbb{Q} . Since X is infinite, there is an injection $\iota : \mathbb{Q} \hookrightarrow X$; then $\mathcal{C} = \{\iota(A_x)\}_{x \in \mathbb{R}}$ is an uncountable linearly ordered family of nonempty subsets of X .

Step 2: For each $A \in \mathcal{C}$, let 1_A be the characteristic function of A . Then $\{1_A\}_{A \in \mathcal{C}}$ is an R -linearly independent set: let $A_1, \dots, A_n \in \mathcal{C}$ and $\alpha_1, \dots, \alpha_n \in R$ be such that $\alpha_1 1_{A_1} + \dots + \alpha_n 1_{A_n} \equiv 0$. We may order the A_i 's such that $A_1 \subset \dots \subset A_n$ and thus there is $x \in A_n \setminus \bigcup_{i=1}^{n-1} A_i$. Evaluating at x gives $\alpha_n = 0$. In a similar manner we find that $\alpha_{n-1} = \dots = \alpha_1 = 0$.

Step 3: Suppose R^X is countably generated: thus there is a surjective R -module map $\Phi : \bigoplus_{i=1}^{\infty} R \rightarrow R^X$. For each $A \in \mathcal{C}$, choose $e_A \in \Phi^{-1}(1_A)$ and put $\mathcal{S} =$

$\{e_A \mid A \in \mathcal{C}\}$. By Step 2, \mathcal{S} is uncountable and R -linearly independent, so it spans a free R -module with an uncountable basis which is an R -submodule of $\bigoplus_{i=1}^{\infty} R$, contradicting Lemma 18. \square

Theorem 20. *If $X \subset R^n$ is infinite, then $E_X : R[t] \rightarrow R^X$ is not surjective.*

Proof. If $E_X : R[t] \rightarrow R^X$ were surjective, then R^X would be a countably generated R -module, contradicting Lemma 19. \square

If $Y \subset X \subset R^n$, restricting functions from X to Y gives a surjective R -algebra map $\tau_Y : R^X \rightarrow R^Y$. Moreover, $E_Y = \tau_Y \circ E_X$. Thus if E_X is surjective, so is E_Y .

Let $\pi_i : R^n \rightarrow R$ be the i th projection map: $\pi_i : (x_1, \dots, x_n) \mapsto x_i$. For a subset $X \subset R^n$, we define the **cylindrical hull** $\mathcal{C}(X)$ as $\prod_{i=1}^n \pi_i(X)$: it is the unique minimal cylindrical subset containing X , and it is finite iff X is.

Proposition 21. *Let $X \subset R^n$ be finite.*

- a) *If $\mathcal{C}(X)$ satisfies Condition (F), then E_X is surjective.*
- b) *If there is a nonempty cylindrical subset $Y = \prod_{i=1}^n Y_i \subset X$ which does not satisfy Condition (F), then E_X is not surjective.*

Proof. a) Since $X \subset \mathcal{C}(X)$, it suffices to show that $E_{\mathcal{C}(X)}$ is surjective, and we have essentially already done this: under Condition (F) we may define $r_X(f) = \sum_{x \in X} f(x) \delta_{X,x}(t)$, and as in § 3.3 we see that $E(r_X(f)) = f$.

b) There is $1 \leq i \leq n$ and $y_i \neq y'_i \in Y_i$ such that $y_1 - y_2 \notin R^\times$, hence a maximal ideal \mathfrak{m} of R with $y_1 - y_2 \in \mathfrak{m}$. For all $j \neq i$, choose $y_j \in Y_j$; let $y = (y_1, \dots, y_n)$; and let y' be obtained from y by changing the i th coordinate to y'_i . For any $f \in F[t]$, $f(y) \equiv f(y') \pmod{\mathfrak{m}}$, so $f(y) - f(y') \in \mathfrak{m}$. Hence the function $\delta_{Y,y} : Y \rightarrow R$ which maps y to 1 and every other element of Y to 0 does not lie in the image of the evaluation map. Thus E_Y is not surjective, so E_X cannot be surjective. \square

Thus if X is itself cylindrical, the evaluation map is surjective iff X satisfies Condition (F): this result is due to Schauz. Proposition 21 is the mileage one gets from this in the general case. When every cylindrical subset of X satisfies condition (F) but $\mathcal{C}(X)$ does not, the question of the existence of interpolation polynomials is left open, to the best of my knowledge even e.g. over \mathbb{Z} .

We say that a ring R is **(F)-rich** (resp. **(D)-rich**) if for all $d \in \mathbb{Z}^+$ there is a d -element subset of R satisfying Condition (F) (resp. Condition (D)). If $\iota : R \hookrightarrow S$ is a ring embedding and R is (F)-rich, then S is (F)-rich, hence also (D)-rich.

Proposition 22. *Let R be a ring and $X \subset R^n$. Consider the following assertions:*

- (i) *E_X is injective.*
- (ii) *X is infinite and Zariski-dense.*
- a) *We always have (i) \implies (ii).*
- b) *If R is (D)-rich – e.g. if it contains an (F)-rich subring – then (ii) \implies (i).*
- c) *If R is finite, a domain, or an algebra over an infinite field, then (ii) \implies (i).*
- d) *If R is an infinite Boolean ring – e.g. $R = \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ – and $X = R^n$, then (ii) holds and (i) does not.*

Proof. a) By contraposition: suppose first that X is finite. Then F^X is a free F -module of finite rank $\#X$ and $F[t]$ is a free F -module of infinite rank, so E cannot be injective. Now suppose X is not Zariski dense: then there is $y \in F^n \setminus X$ and

- $f \in F[t]$ such that $E(f)|_X \equiv 0$ and $E(f)(y) \neq 0$, hence $0 \neq f \in \text{Ker } E$.
- b) Let $f \in \text{Ker } E_X = I(X)$, and let $d = \deg f$. Since X is Zariski-dense in F^n , $f(x) = 0$ for all $x \in F^n$. Since R is (D)-rich, there is a $S \subset R$ of cardinality $d + 1$ satisfying Condition (D). Put $X = \prod_{i=1}^n S$. Then $f \in \mathcal{R}_X$ and $f(x) = 0$ for all $x \in X$, so $f = 0$ by Theorem 11.
- c) This is immediate from part b).
- d) Since R is infinite, R^n is infinite and Zariski-dense. Since R is Boolean, the polynomial $t_1^2 - t_1$ evaluates to zero on every $x \in R^n$. \square

Acknowledgments: My interest in Combinatorial Nullstellensätze and connections to Chevalley's Theorem was kindled by correspondence with John R. Schmitt. The main idea for the proof of Lemma 19 is due to Carlo Pagano. I thank Emil Jeřábek for introducing me to the Finite Field Nullstellensatz.

REFERENCES

- [Al99] N. Alon, *Combinatorial Nullstellensatz*. Recent trends in combinatorics (Mátraháza, 1995). *Combin. Probab. Comput.* 8 (1999), 7-29.
- [AT92] N. Alon and M. Tarsi *Colorings and orientations of graphs*. *Combinatorica* 12 (1992), 125-134.
- [Br87] W.D. Brownawell, *Bounds for the degrees in the Nullstellensatz*. *Ann. of Math.* (2) 126 (1987), 577-591.
- [Br11] D. Brink, *Chevalley's theorem with restricted variables*. *Combinatorica* 31 (2011), 127-130.
- [CFS14] P.L. Clark, A. Forrow and J.R. Schmitt, *Warning's Second Theorem with Restricted Variables*. <http://arxiv.org/abs/1404.7793>
- [Ch35] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*. *Abh. Math. Sem. Univ. Hamburg* 11 (1935), 73-75.
- [EMR] T. Y. Lam, *Exercises in modules and rings*. Problem Books in Mathematics. Springer, New York, 2007.
- [Ko88] J. Kollár, *Sharp effective Nullstellensatz*. *J. Amer. Math. Soc.* 1 (1988), 963-975.
- [KP12] R.N. Karasev and F.V. Petrov, *Partitions of nonzero elements of a finite field into pairs*. *Israel J. Math.* 192 (2012), 143-156.
- [L] S. Lang, *Algebra*. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.
- [La10] M. Lasoń, *A generalization of combinatorial Nullstellensatz*. *Electron. J. Combin.* 17 (2010), Note 32, 6 pp.
- [LMR] T. Y. Lam, *Lectures on modules and rings*. Graduate Texts in Mathematics, 189. Springer-Verlag, New York, 1999.
- [Sc08] U. Schauz, *Algebraically solvable problems: describing polynomials as equivalent to explicit solutions*. *Electron. J. Combin.* 15 (2008), no. 1, Research Paper 10, 35 pp.
- [Ta13] T. Tao, *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*, preprint.
- [Te66] G. Terjanian, *Sur les corps finis*. *C. R. Acad. Sci. Paris Sér. A-B* 262 (1966), A167-A169.